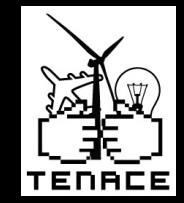
UNIVERSITY OF TRENTO

SECONOMICS



How CVSS is DOSsing your patching policy (and wasting your money)

Luca Allodi, Fabio Massacci
University of Trento, Italy.

Who are we?

- Security Group at the University of Trento (Italy)
- Coordinates many M€ European R&D Projects on
  - CYBER SECURITY
  - ECONOMICS OF IT SECURITY
  - SECURITY ENFORCEMENT
  - We work with:
    - International Airports, Metropolitan Transport,
    - UK/US National Grid, SAP, Symantec, Atos..
- More details at
  - http://securitylab.disi.unitn.it

A small presentation disclaimer

- We'll often use **medical examples** to clarify some ideas on testing for "gravity of illnesses/vulns"..
- … and Fabio's the only doctor on stage
- When you see **this logo** it means Fabio will follow from next slide in a more.. "medical fashion"

- ..So, let's start now

Vulnerabilities: an (expensive) question

- What the CIO really wants to know:
  - About that new vulnerability everybody talks about..
  - Should I worry?
- Ask a guru..
  - "Security is only as strong as the weakest link". B. Schneier
  - "One vulnerability after another has been discovered and exploited by criminals" R. Anderson
- Ask NIST..
  - U.S. Gov. Mandates Security Management tools to use CVSS score to assess software vulnerabilities

Fix all HIGH CVSS vulnerabilities or die

Ask your doctor

- I have a sw with a vulnerability…
- Is it easy to access?
- Is it high impact?
- Your CVSS doctor says HIGH → patch
  - ✓ Of course please…

- I see double…
- Both eyes involved?
- Primary gaze impacted?
- Your CVSS doctor says brain surgery
  - ? Ehm are you sure…

CVSS is a test by clinical expertise, how informative is it?

Tests and Risks

- A clinical test must be matched to the risk
  - Binocular diplopia →42% recovered ***without*** treatment
  - Binocular diplopia AND intracranial lesion → 0% recovered without treatment
    - Nolan "Diplopia" B. J. Ophtalm. 1966
- What the CIO would like to know:
  - IF HIGH CVSS listed by Sec. Config. Manager and Metasploit finds it → fix it and decrease risk by +15%
  - IF fix all remaining HIGH listed by Sec. Config. Manager → changes from 15% to 18%
  - → Is +3% worth the extra money?

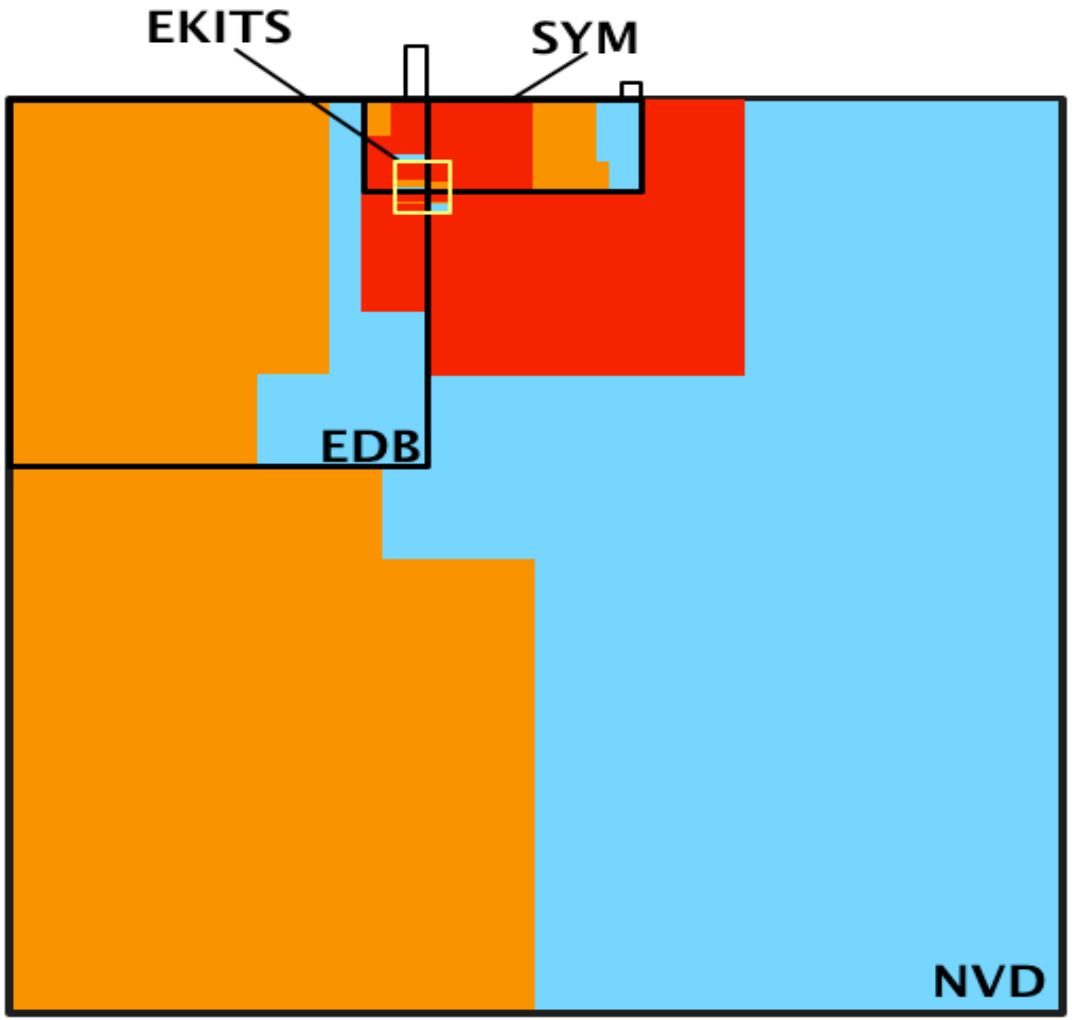
Attacks: Two Options

- You are THE Target
  - can mitigate this risk (IDSs, DLP, other Remediation strategies, insurance, etc.)
  - But can't control everything
  - → speaking of "risk decrease by X%" doesn't make sense
- You are ONE of the Targets
  - Automated exploitation, phishing sites etc.
  - GOOGLE: 80% of attacks are of this nature
    - M. Rajab et al., Google Tech Report 2011
  - For these threats → "risk decrease by x%" makes sense
- We do not focus on Black Swan events
- → We focus on the most common threats

Vulnerabilities: our baseline

- NATIONAL VULNERABILITY DATABASE: NVD – 49.624 vulns
  - The universe of vulnerabilities
- WHITE MARKETS OF EXPLOITS: EXPLOIT-DB – 8.189 vulns
  - Proof-of-Concept exploits published by security researchers
- ACTUAL EXPLOITS IN THE WILD: SYM – 1.274 vulns
  - Symantec / Kaspersky Threat reports
  - Vulnerabilities actually exploited in the wild
  - Conservative approach: SYM represents the existence of an attack
  - Browser/Plugins 14% – Server 22% – App. 17% - Windows 13%
  - Other OS 5% - Developer 5% - Business 7% - Unclassified 17%
- BLACK MARKETS FOR EXPLOITS: EKITS – 114 vulns
  - 2/3 of client threaths according Google (2011)
  - Exploit advert from the bad guys in an exploit kit
  - 90+ exploit kits from the black markets expanding Contagio's exploit pack table

CVSS Study: Map of Vulns



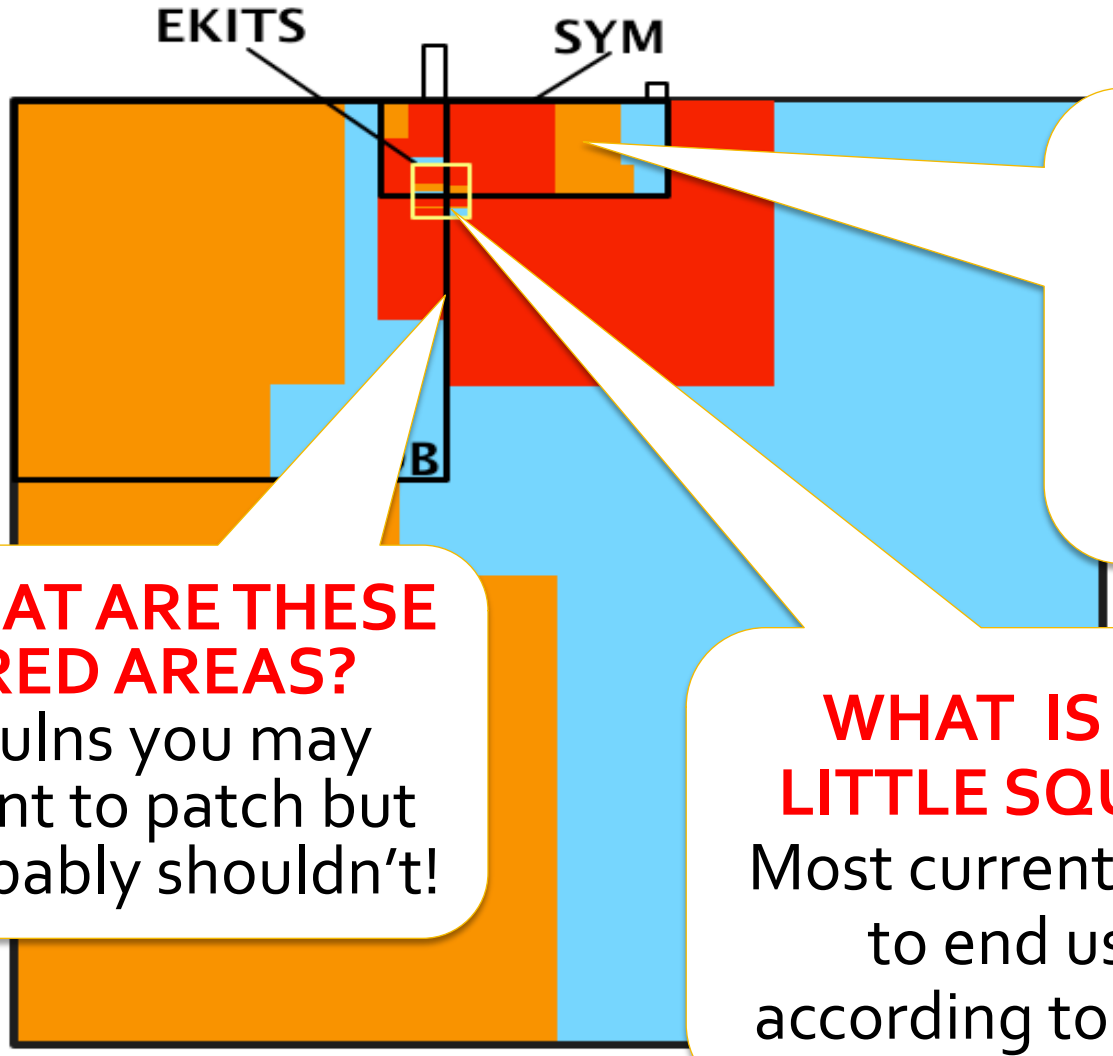
LOW CVSS<6

6≤MEDIUM CVSS<9

HIGH CVSS ≥ 9

Areas are proportional to no. of vulns

CVSS Study: Map of Vulns

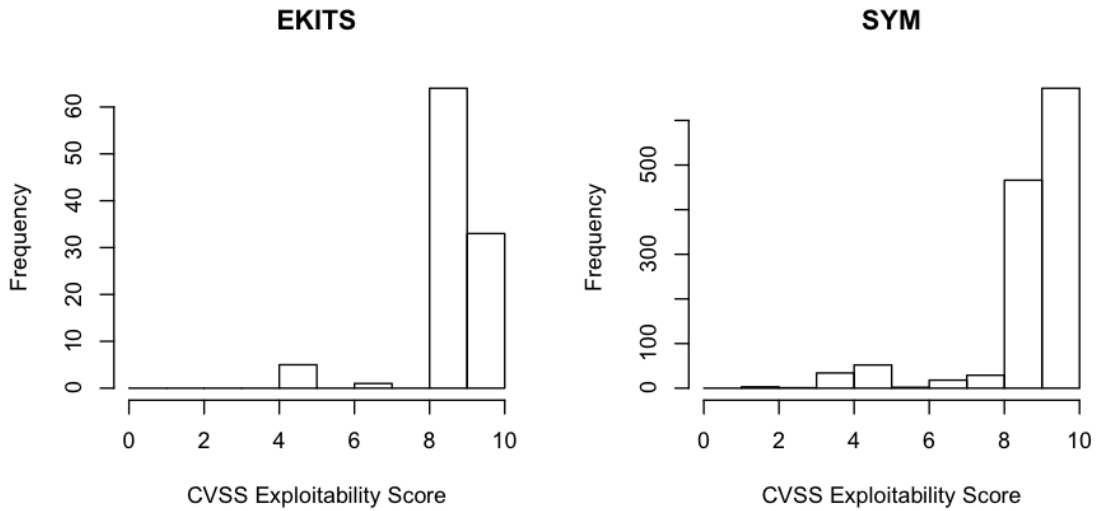


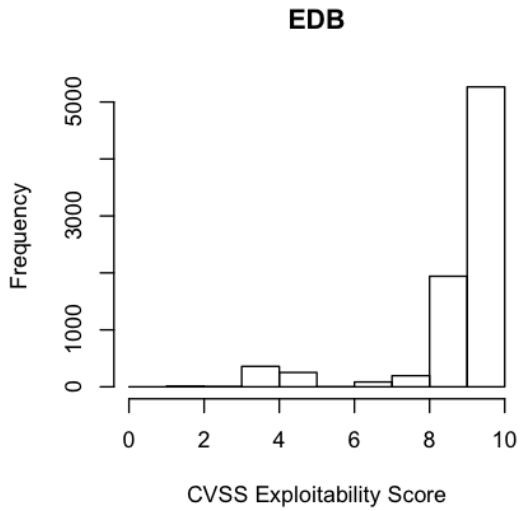
WHAT IS THIS?
50% of attacked vulns you did not patch

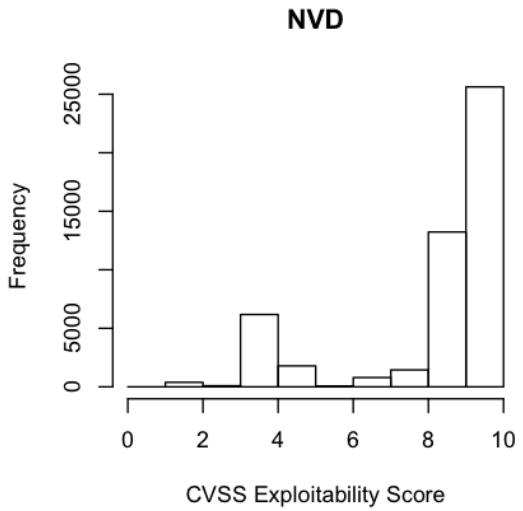
WHAT ARE THESE RED AREAS?
Vulns you may want to patch but probably shouldn't!

WHAT IS THIS LITTLE SQUARE?
Most current threats to end users according to Google

What makes CVSS so inaccurate?







- Risk (CVSS)= Impact x Likelihood
  - CVSS Likelihood = Exploitability
- Everything is exploitable → CVSS lacks of a real measure of likelihood of exploitation
- Impact is the only real measure
- ..CVSS is not estimating risk


Hey, I don't agree!

- You say CVSS is not a good measure.. But you can't do statistics on NVD!! Because..
- NVD contains:
  - Lots of old vulnerabilities!
  - Lots of entries for software almost nobody uses
- EDB contains:
  - Lots of software that SYM does not monitor
    - True: EDB ~5500 sw entries not in SYM vs 333 in both
- … So we need something more precise

Do High CVSS scores predict attacks?

- Do smoking habits predict cancer?
  - → You can't ask people to start smoking so you can't run a controlled experiment → same here
- Case controlled study
  - Cases: people with lung cancer
  - Possible confounding variables
    - Age, Sex, Social Status, Location
  - Explanatory variable
    - Smoking habit
- For each of the cases select another person with the same values of the control variables
  - Doll & Bradfor Hill, British Medial Journal 1950

CVSS Case Controlled Experiment I

You observe..	In subjects from ..	Categorized by…	And you think that's because they:
Lung Cancer	Same Hospital Patients	• Age • Sex • Location	• Smoke a lot • Smoke • Don't smoke
Exploitation	Same kind of exploitable vulnerabilities	• Confidentiality • Integrity • Avail • Year • Affected software	• CVSS is HIGH • CVSS is LOW • Vuln is in EDB • Vuln is in EKITS

CVSS Case Controlled Experiment II

- Case:
  - CVE-2010-3962 (use-after-free vulnerability in MS IE 6,7,8)
  - Year=2010
  - Confidentiality =C, Integrity=C, Availability=C
  - Vendor=Microsoft, Software = ie
- Control: select 1 out of
  - 5 from EKITS
  - 7 from EDB
  - 37 from NVD
- Repeat for all 1274 cases in SYM
  - See what values of CVSS we get
  - See how many times we get back in SYM

CVSS Case Controlled Experiment III

- Sensitivity → true positives vs all sick people
  - HIGH→ the test correctly identifies exploited vulns
  - LOW → lots of "sick people" undetected

- Specificity → true negatives vs all healthy people
  - HIGH → the test correctly identifies non exploited vulns
  - LOW → lots of "healthy people" flagged

Security Rating as a "Generate Panic" test

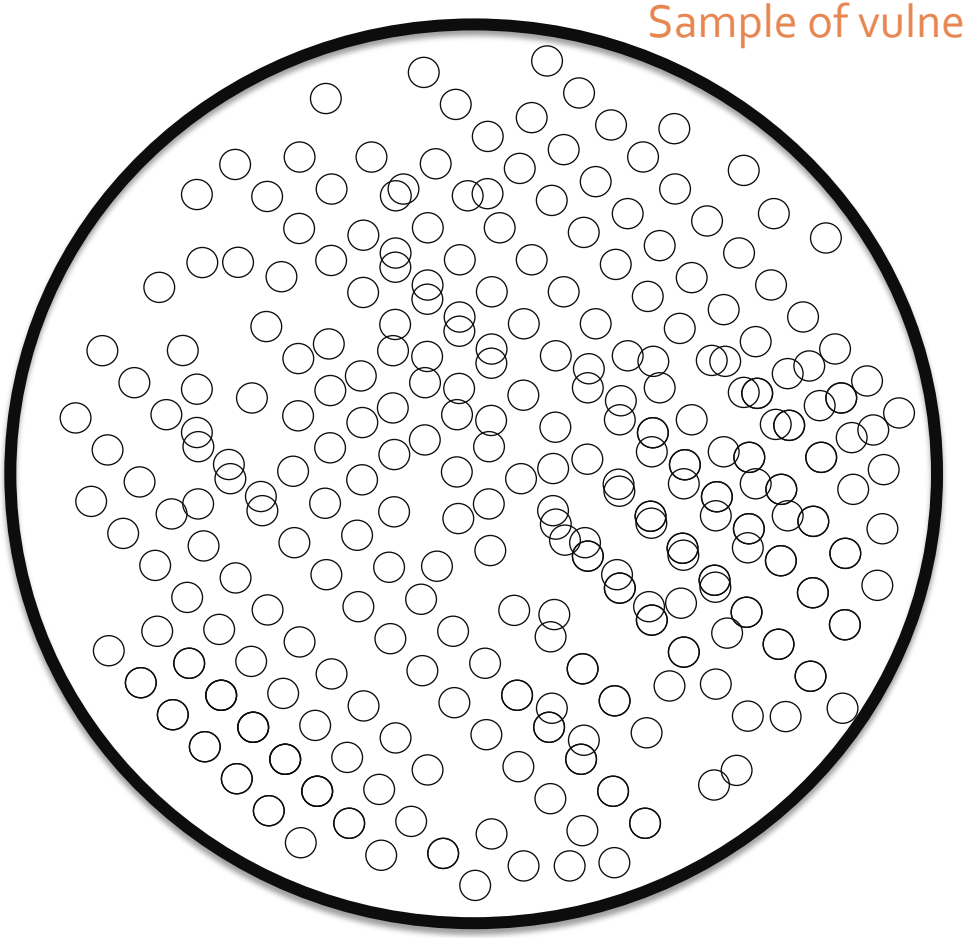
- Sensitivity: is High/Med CVSS good marker for v∈SYM?
- Specificity: is Low CVSS good marker for v∉SYM?

Test for Patching	Sensitivity	Specificity
Patch Everything	100%	0%
CVSS High+Med	91%	23%
CVSS + PoC in EDB	97%	22%
CVSS + EKITS	94%	50%
3BT: Down Syndrome	69%	95%
PSA: Prostate Cancer	81%	90%


Let's plug this in into your patching schedule

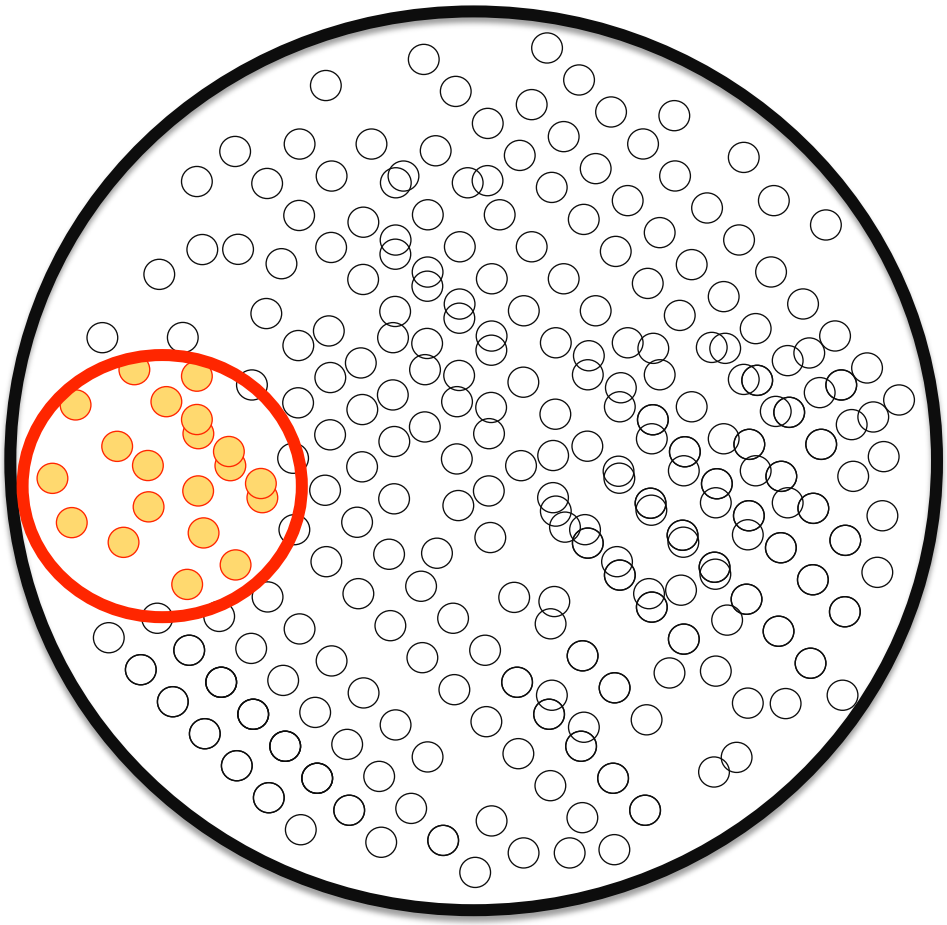
- Assume you want to patch HIGH and MED CVSS
  - and (optimistic) patching cost is proportional to number of vulns
- Specificity 22% (1/4)? → you spend 300-400% more than you should (at least)
- But how many attacks will you avoid in practice?
- Patch HIGH and MED scores. Remember..
  - Sensitivity = Prob attacked vuln gets HIGH or MED score = 90.9%
  - 1- Specificity = Prob non-attacked vuln gets HIGH or MED score = 1-0.2272 = 77.28%
  - Pr(attacked | patched) -> Bayes Theorem, etc..
  - → 9 out of 10 to-patch vulns could stay as they are
- Can't believe it? Let's visualize it

Visualizing a Patching Strategy



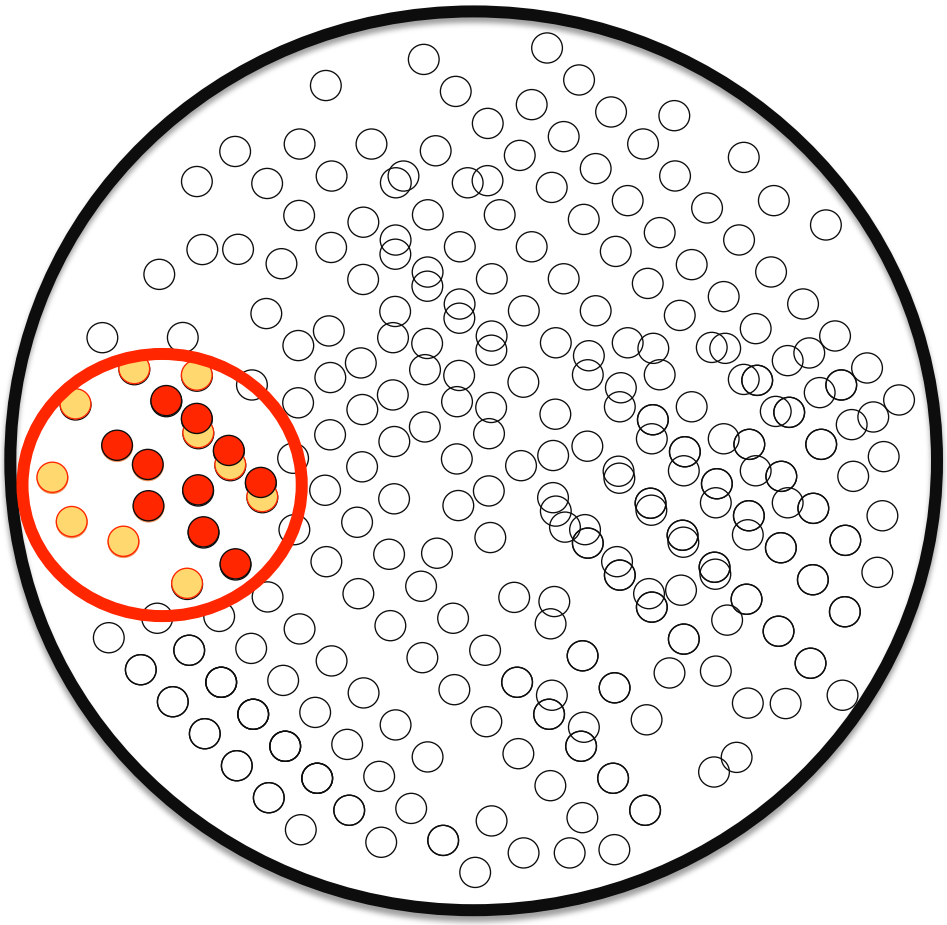

Visualizing a Patching Strategy II

Attacked vulns in a sample (4.3%)



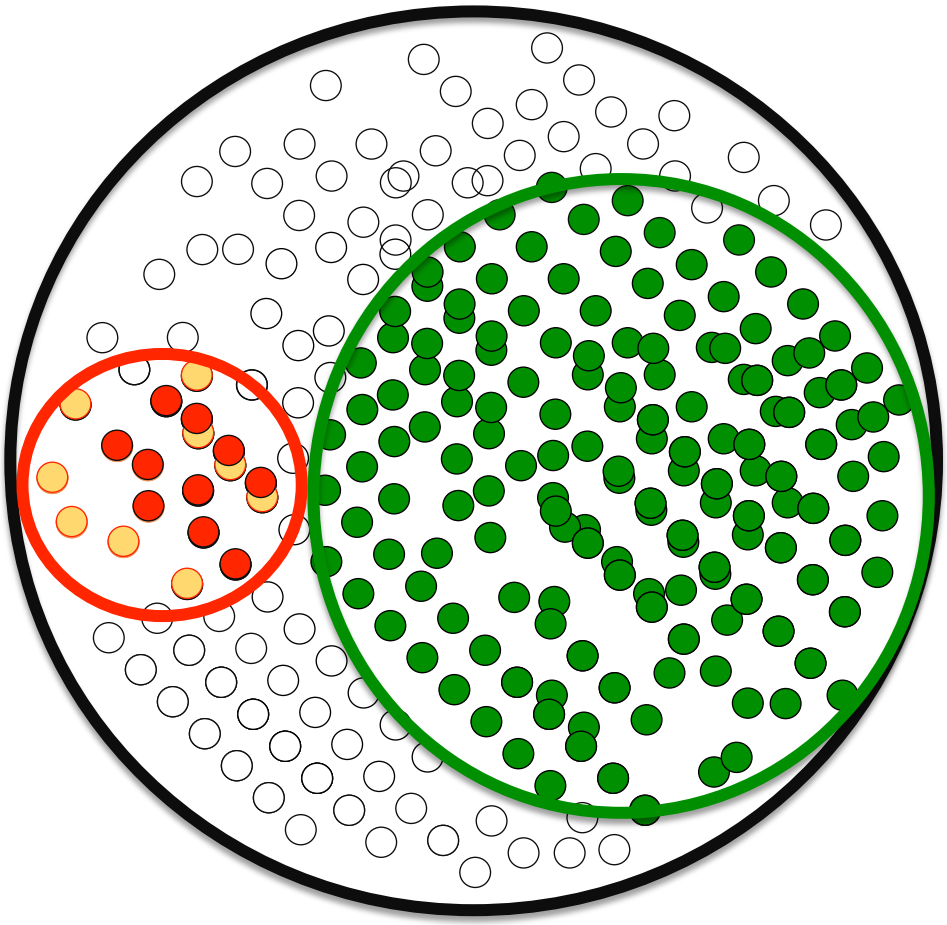
Visualizing a Patching Strategy III

90.9% of attacked Vulns are scored HIGH or MED



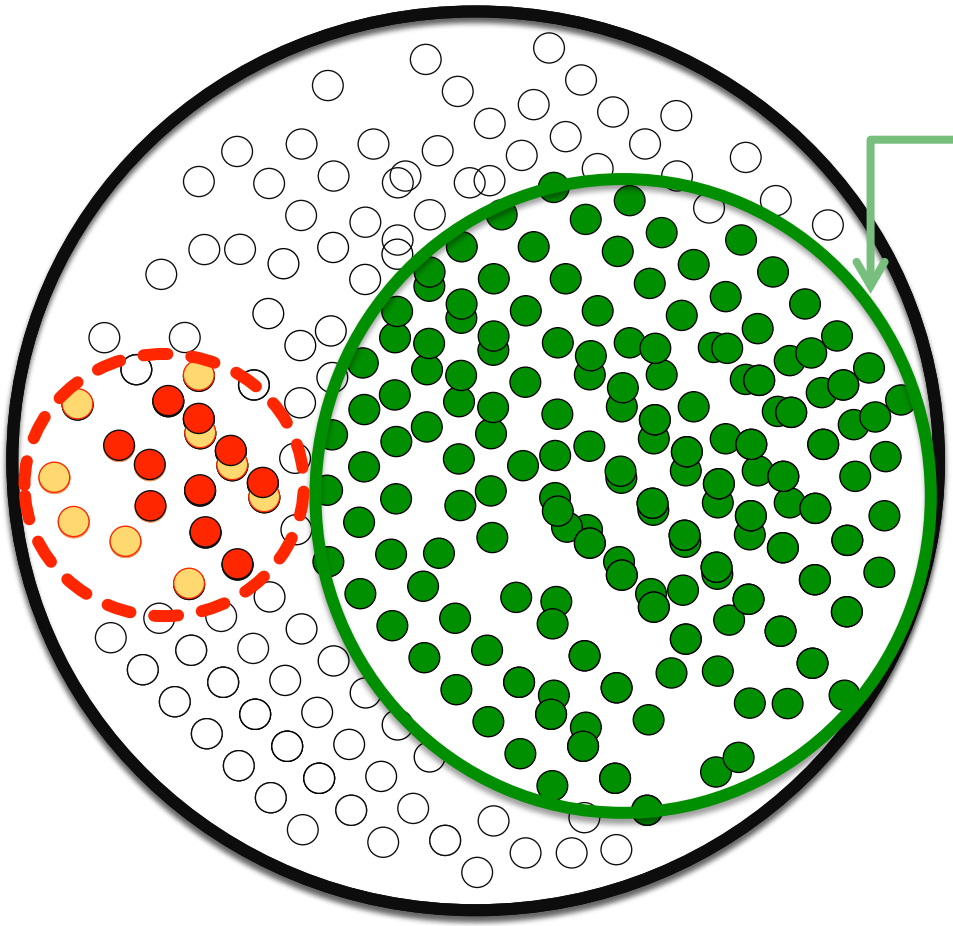
Visualizing a Patching Strategy IV

77.2% of NON attacked Vulns are scored HIGH or MED



Visualizing a Patching Strategy V

94-95% of to-patch vulns may probably just be skipped




Conclusion: answer to the CIO

- Is wearing a seat belt any useful?
  - Pr(Death x Safety Belt on) – Pr(Death x Safety Belt off)
  - Yes it is→ 43% improvement of chances of survival
    - L. Evans, Accident Analysis and Prevention 1986
- Is patching HIGH score any useful?
  - Pr(Attack x CVSS High) – Pr(Attack x CVSS Low)
- Finally the figures the CIO wants
  - Patching HIGH/MED and exploit sold in Exploit Kits
    →improves by +62.81% (Buckle up!)
  - Patching fix HIGH/MED and PoC exploit by white hats
    → improves by +19.64% (Up to you)
  - Patching just HIGH/MED
    → improves by +3.2% (Life is too short)

Thanks